UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/571,048	03/03/2006	Kazuki Ogawa	FUJY 22.426	1755

26304   7590   08/06/2009
KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER
JIMENEZ, DANILO

ART UNIT	PAPER NUMBER
2447	

MAIL DATE	DELIVERY MODE
08/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _03 March 2006_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-14_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-14_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _03 March 2006_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
        1.☐ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _3/3/2006_.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____ .

DETAILED ACTION

1.   The claims 1-14 are pending.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.   Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Wiegel

(U.S. Patent No. 6,484,261 B1).

        With respect to claim 1, Wiegel teaches a policy control device for reflecting a

policy rule defined by a condition and an action corresponding to the condition for

operation setting of respective network devices present in a network to be managed,

according to a transition of operation states of the network (i.e., network management

systems address this general need to monitor the status of a device in the network, a

network management station transmits a message requesting information to a software

program or agent running on the target device. In response, the agent sends a message

back to the network management station, column 3 lines 59-64), comprising: a storage

unit for storing a plurality of multi-policy rules generated in units of combination of at

least two single policy rules having different actions on the same condition, together

with particular information of a network device to be applied, in such a manner that the

plurality of multi-policy rules and the particular information can be updated (i.e., the

network devices enforce the security policies. The functions of network devices such as

switches and routers include receiving packets of data, and determining whether to

forward each packet to another device or location, or to refuse to forward a packet. The

particular way that these functions operate is determined, in part, by control instructions

stored in the network device. Policies are constructed in memory during an editing

session in which an administrator works with the graphical user interface. The

administrator indicates that editing is complete by initiating a File Save command. In

response, the policy and its associated script are saved in a database, column 1 lines

55-61 and column 14 lines 20-24); and a control unit for applying one of the plurality of

multi-policy rules stored in the storage unit for the operation setting of the network

device identified, based on the particular information. (i.e., a method for controlling a

network device that passes or rejects information messages, by defining a set of

symbols that identify logical operations that can be carried out by the network device;

defining an information communication policy for the network device by graphically

interconnecting one or more of the symbols into a symbolic representation of the policy;

and generating a set of instructions based on the symbolic representation of the policy,

wherein the set of instructions causes the network device to selectively pass or reject

messages according to the policy, column 5 lines 12-23).

With respect to claim 2, Wiegel teaches a policy control device for reflecting a

policy rule defined by a condition and an action corresponding to the condition for

operation setting of respective network devices present in a network to be managed,

according to a transition of operation states of the network (i.e., network management

systems address this general need to monitor the status of a device in the network, a

network management station transmits a message requesting information to a software

program or agent running on the target device. In response, the agent sends a message

back to the network management station, column 3 lines 59-64), comprising: a storage

unit for storing a plurality of single policy rules having different actions on the same

condition, together with particular information of a network device to be applied and

application priority information, in such a manner that the plurality of single policy rules,

the particular information and the application priority information can be updated (i.e.,

the network devices enforce the security policies. The functions of network devices such

as switches and routers include receiving packets of data, and determining whether to

forward each packet to another device or location, or to refuse to forward a packet. The

particular way that these functions operate is determined, in part, by control instructions

stored in the network device. Policies are constructed in memory during an editing

session in which an administrator works with the graphical user interface. The

administrator indicates that editing is complete by initiating a File Save command. In

response, the policy and its associated script are saved in a database, column 1 lines

55-61 and column 14 lines 20-24); and a control unit for applying one of the plurality of

single policy rules stored in the storage unit for the operation setting of the network

device identified, based on the particular information according to an order of priority,

based on the priority information (i.e., a method for controlling a network device that

passes or rejects information messages, by defining a set of symbols that identify

logical operations that can be carried out by the network device; defining an information

communication policy for the network device by graphically interconnecting one or more

of the symbols into a symbolic representation of the policy; and generating a set of

instructions based on the symbolic representation of the policy, wherein the set of

instructions causes the network device to selectively pass or reject messages according

to the policy, column 5 lines 12-23).

With respect to claim 3, Wiegel teaches wherein: the condition contains at least

one selected from among a line trouble, an excess of a traffic amount threshold value,

and an excess of a packet loss threshold value each indicating operation states of the

network to be managed (i.e., administrators actually define security policies that control

the traffic leaving the site, column 31 lines 40-43. Wherein, a threshold value of traffic

can be set.); and the action contains at least two selected from among switching of a

traffic flow path, flow control for suppressing traffic, and a notification to a network

operator (i.e., by controlling which "sessions" can occur between two network objects, a

gateway or firewall that uses the present system secures the flow of network traffic.

The system may also include a monitor agent that is responsible for monitoring,

reporting, and notification about the security status of the other agents that surround the

knowledge base, column 9 lines 46-60 and column 11 lines 30-42).

With respect to claim 4, Wiegel teaches wherein the particular information of the network device to be applied contains identification information of the network device and identification information of a line interface (i.e., a router is programmed using a set of router rules that determine whether the router should forward or reject packets based upon the type of packet, originating network location, destination location, and other criteria. The following example presents a rule set used to program a router to allow traffic across it for an anonymous file transfer protocol (FTP) server that resides on a network object having an Internet Protocol (IP) address of 192.10.1.2., column 2 lines 7-18).

With respect to claim 5, Wiegel teaches wherein each of the plurality of multi-policy rules is generated in units of combination of at least two of the single policy rules having the different actions on the same condition preregistered in the storage unit, to enable hierarchical management of the plurality of multi-policy rules (i.e., if the parameters of a session request match two security policies within a direct path, the policy attached to the most specific network object defined in that path is applied to that session. The rules for policy inheritance are processed according to the hierarchical arrangement of the Networks tree, column 28 lines 26-35).

With respect to claim 6, Wiegel teaches wherein: the storage unit further stores application priority information of the plurality of multi-policy rules in such a manner that

the application priority information can be updated (i.e., the steps of dynamically

updating the set of instructions as the information communication policy is defined. The

method further includes the steps of storing a decision tree comprising one or more

nodes, in which the decision tree represents a logical flow of commands that are to be

executed by the network device; and inserting a node into a decision tree, wherein the

node is associated with a symbol that is added to the policy, column 5 lines 41-51 and

column 5 lines 61-66); and the control unit applies one of the plurality of multi-policy

rules for the operation setting of the network device, according to an order of priority

based on the priority information (i.e., a related feature is that the step of generating the

set of instructions comprises the steps of dynamically updating the set of instructions as

the symbolic representation is re-configured. It provides a method for controlling a

network device that passes or rejects information messages, by defining a set of

symbols that identify logical operations that can be carried out by the network device;

defining an information communication policy for the network device by graphically

interconnecting one or more of the symbols into a symbolic representation of the policy;

and generating a set of instructions based on the symbolic representation of the policy,

wherein the set of instructions causes the network device to selectively pass or reject

messages according to the policy, column 5 lines 41-51 and column 5 lines 12-23).

With respect to claim 7, Wiegel teaches wherein: the storage unit further stores

application priority information of the single policy rules in each of the plurality of multi-

policy rules in such a manner that the application priority information can be updated

(i.e., the steps of dynamically updating the set of instructions as the information communication policy is defined. The method further includes the steps of storing a decision tree comprising one or more nodes, in which the decision tree represents a logical flow of commands that are to be executed by the network device; and inserting a node into a decision tree, wherein the node is associated with a symbol that is added to the policy, column 5 lines 41-51 and column 5 lines 61-66); and the control unit applies the single policy rules in each of the plurality of multi-policy rules for the operation setting of the network device, according to an order of priority based on the priority information (i.e., a related feature is that the step of generating the set of instructions comprises the steps of dynamically updating the set of instructions as the symbolic representation is re-configured. It provides a method for controlling a network device that passes or rejects information messages, by defining a set of symbols that identify logical operations that can be carried out by the network device; defining an information communication policy for the network device by graphically interconnecting one or more of the symbols into a symbolic representation of the policy; and generating a set of instructions based on the symbolic representation of the policy, wherein the set of instructions causes the network device to selectively pass or reject messages according to the policy, column 5 lines 41-51 and column 5 lines 12-23).

The limitations of claim 8 are rejected in the analysis of claim 1 above, and the claim is rejected on that basis.

The limitations of claim 9 are rejected in the analysis of claim 2 above, and the claim is rejected on that basis.

The limitations of claim 10 are rejected in the analysis of claim 3 above, and the claim is rejected on that basis.

The limitations of claim 11 are rejected in the analysis of claim 4 above, and the claim is rejected on that basis.

The limitations of claim 12 are rejected in the analysis of claim 5 above, and the claim is rejected on that basis.

The limitations of claim 13 are rejected in the analysis of claim 6 above, and the claim is rejected on that basis.

The limitations of claim 14 are rejected in the analysis of claim 7 above, and the claim is rejected on that basis.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANILO JIMENEZ whose telephone number is (571) 270-7218. The examiner can normally be reached on Monday - Friday 7:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Hwang can be reached on (571) 272-4036. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DANILO JIMENEZ
Examiner, Art Unit 2447
July 31, 2009

/Joon H. Hwang/
Supervisory Patent Examiner, Art Unit 2447